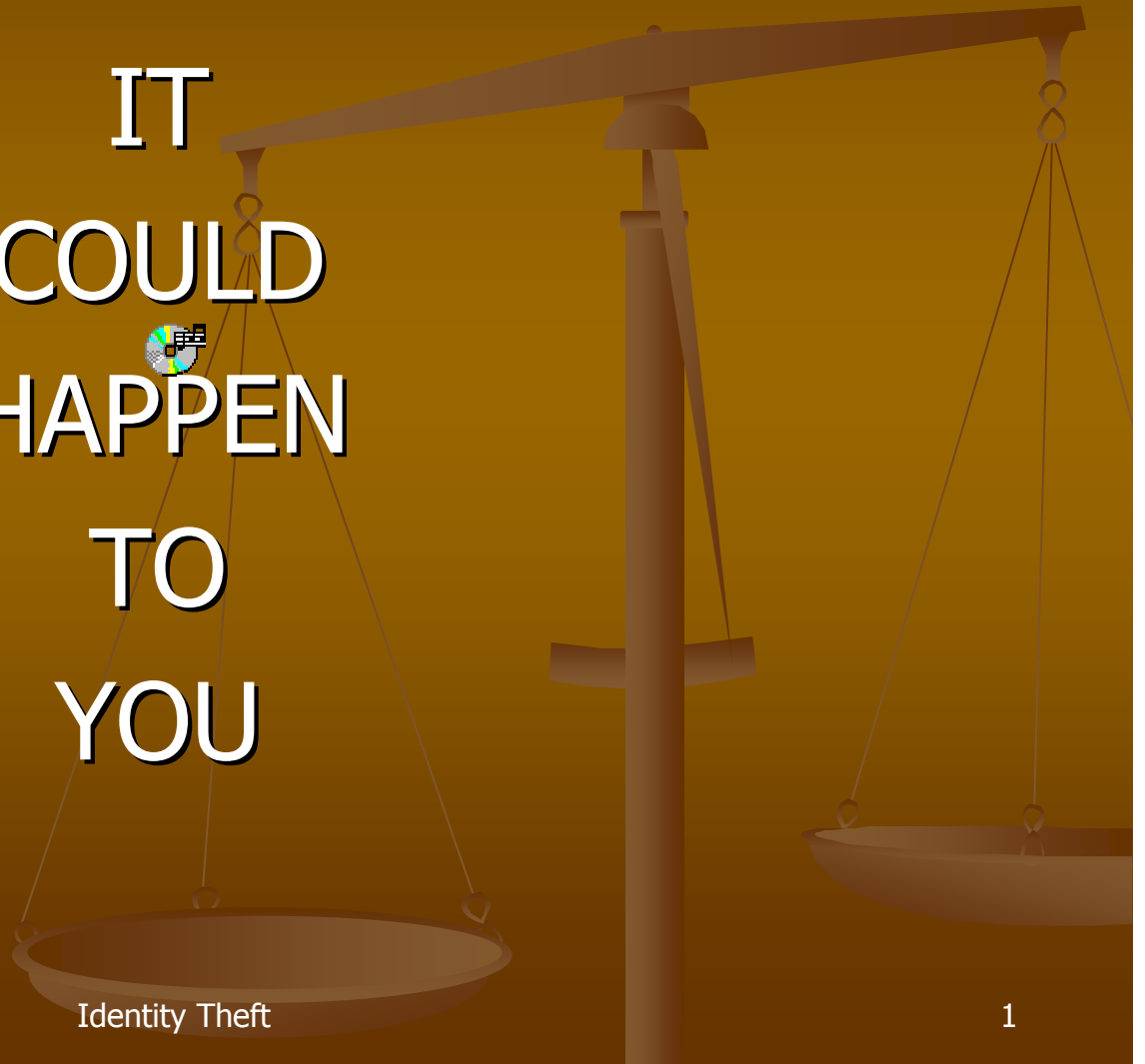


# IDENTITY THEFT

IT  
COULD  
HAPPEN  
TO  
YOU



10/1/2007

Identity Theft

1

# IDENTITY THEFT



Kevin P. Kelly – Director of Queensborough Taxpayer Outreach Program (Q-TOP), Attorney at Law, Certified Public Accountant and an Assistant Professor.

James C. McMahon – Co.- Director of Queensborough Taxpayer Outreach Program (Q-TOP), Attorney at Law.

# Identity Theft



1. Identity Theft Statistics.
2. Identity Theft Penalty Enhancement Act.
3. Different Ways Identity Theft Occurs.
4. Be Alert to Possible Identity Theft.
5. How to Safeguard Information.
6. Steps to Protect Against Identity Theft.

# Identity Theft

## *Identity Theft Statistics*

According to the FBI Identity Theft is the fastest growing crime in the United States. Identity theft in 2003 was the second most reported crime to the Federal Government.

The Federal Trade Commission Recorded:

- 161,836 consumer fraud complaints of Identity Theft in 2002.
- In 2003 that number increased to 214,905
- A September 2003 FTC survey found that 27.3 million Americans had been victims of some form of Identity Theft within the past five years.

# Identity Theft

- The largest Identity Theft scam in history occurred in New York. The theft scam involved the theft of credit histories of 30,000 victims costing 2.7 million dollars. They used the stolen information to charge large sums to credit card numbers, empty bank accounts and obtain fraudulent loans.
- Gartner Research of Stanford, Conn. found that between April 2003 and April 2004 Phishing Victims alone lost 1.2 Billion dollars to Identity Theft.
  - Phishing is an online scam where consumers are duped into entering personal data on counterfeit Banking and E. Commerce websites.

# Identity Theft

## **Identity Theft Laws**

The Identity Theft Penalty Enhancement Act Amended Chapter 47 of Title 18, of the United States Code by adding:

### **Sec. 1028A. Aggregated Identity Theft**

#### (a) Offense

- (1) In general – Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.
- (2) Terrorism Offense – Whoever, during and in relation to any felony violation enumerated in section 2332b(g)(5)(B), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person or a false identification document shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 5 years.

# Identity Theft

(b) Consecutive Sentence – Notwithstanding any other provision of law—

- (1) a court shall not place on probation any person convicted of a crime in this section;
- (2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other provision of law, including any term of imprisonment imposed for the felony during which the means of identification was transferred, possessed, or used;

# Identity Theft

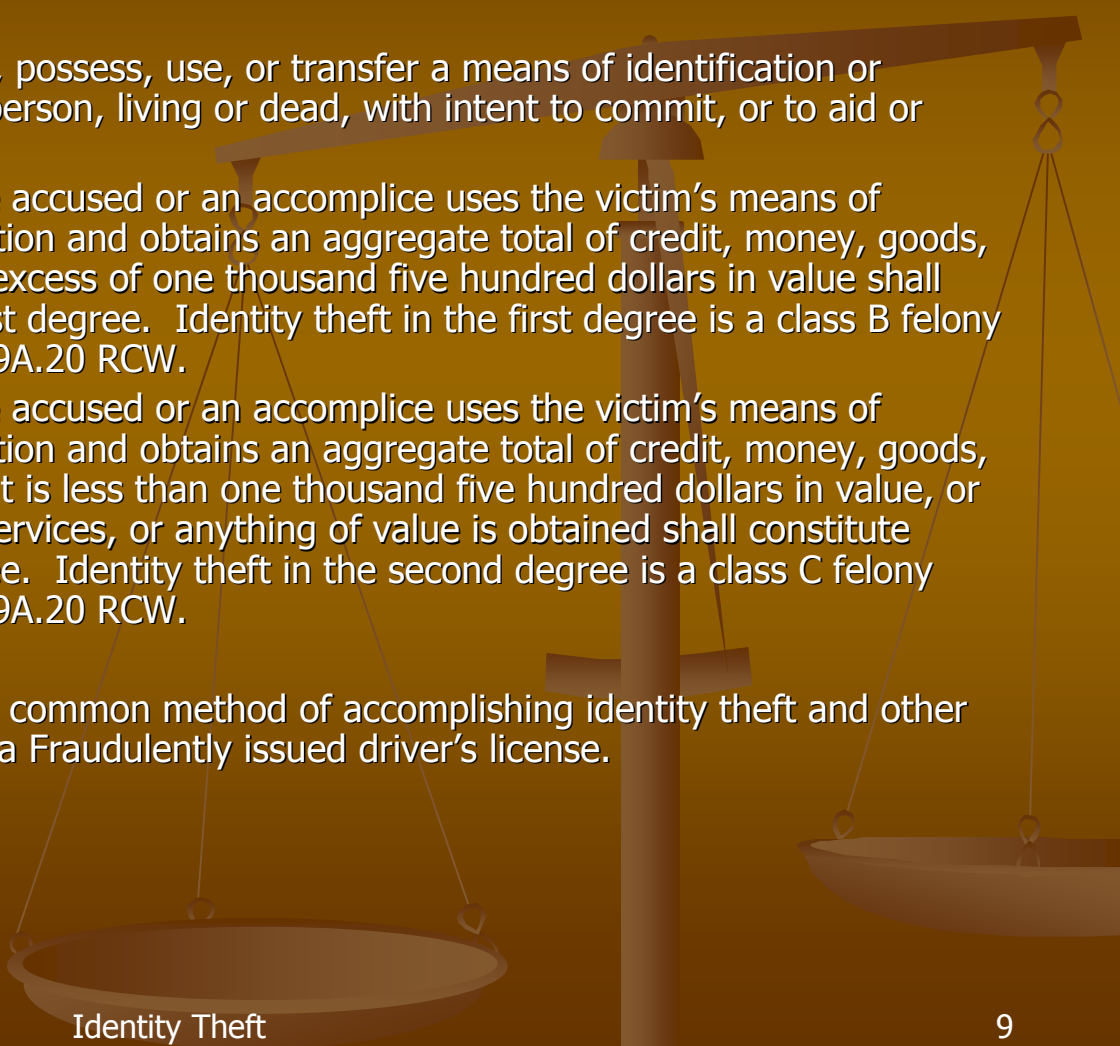


- (3) in determining any term of imprisonment to be imposed for the felony during which the means of identification was transferred, possessed, or used, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and
- (4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term or imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the Sentencing Commission pursuant to section 994 of Title 28.



# Identity Theft

## Washington State RCW 9.35.020 Identity Theft

- 
- (1) No person may knowingly obtain, possess, use, or transfer a means of identification or financial information of another person, living or dead, with intent to commit, or to aid or abet, any crime.
  - (2) Violation of this section when the accused or an accomplice uses the victim's means of identification or financial information and obtains an aggregate total of credit, money, goods, services, or anything of value in excess of one thousand five hundred dollars in value shall constitute identity theft in the first degree. Identity theft in the first degree is a class B felony punishable according to chapter 9A.20 RCW.
  - (3) Violation of this section when the accused or an accomplice uses the victim's means of identification or financial information and obtains an aggregate total of credit, money, goods, services, or anything of value that is less than one thousand five hundred dollars in value, or when no credit, money, goods, services, or anything of value is obtained shall constitute identity theft in the second degree. Identity theft in the second degree is a class C felony punishable according to chapter 9A.20 RCW.

Washington found that the most common method of accomplishing identity theft and other fraudulent activity is by securing a Fraudulently issued driver's license.

# Identity Theft

## **New York State Penal Law**

Section 190.77 – 190.84: Defines Identity Theft as an unlawful possession of personal Identification Information.

Sec 190.77 – Offenses involving theft of identity; definitions.

Sec 190.78 - Identity Theft in the third degree.

Sec 190.79 - Identity Theft in the second degree.

Sec 190.80 - Identity Theft in the first degree.

Sec 190.81 - Unlawful possession of personal identification information in the third degree.

Sec 190.82 - Unlawful possession of personal identification information in the second degree.

Sec 190.83 - Unlawful possession of personal identification information in the first degree.

Sec 190.84 - Defenses.

# IDENTITY THEFT



- **MEYERSON v. PRIME REALTY SERVS., LLC**, 2005  
NYSLIP 25078, 2/28/05 SUMPEME COURT, N.Y. COUNTY

Landlord requests Tenant to complete form with Social Security #.  
stating Tenant has legal obligation to do so.  
Tenant refuses; Landlord threatens eviction.

Court reviews legal history of confidentiality of Social Security #'s.

Court relies on threat of eviction as “deceptive practice” under  
consumer protection law to uphold refusal to provide Social Security  
number.

# Identity Theft

- **Altegra Credit Co. v. Tin Chu**, 2004 NY Slip OP 50241(U), 3/25/04 (Supreme Court, Kings County).
- Tin Chu & Mona business deal; no \$ from Mom.
- Mom notices lots of strange unopened mail showing up at house for Tin Chu.
- Mortgage foreclosure & criminal case against Tin Chu;
- Forgery of deed & theft of mortgage proceeds.
- Title insurance company litigates based on photo of passport produced at mortgage closing.
- Ultimately Mom prevails.

# Identity Theft

- ***Daly v. Metropolitan Life Ins. Co.,***
- 2004 NY SlipOP 24280,5/20/04.
- (Supreme Court, N.Y. Co.)
- Application for insurance policy.
- Application information stolen from Met Life office by employee of cleaning service which cleans Met Life office.
- Numerous credit card accounts opened in name of plaintiff and her father.

# Identity Theft



- Daly v. Metropolitan Life-continued.
- “Covenant of trust and confidence may be inferred in business dealings.”
- Met Life seeks dismissal of Complaint claiming it was not negligent.
- Court says the case must go to trial.
- [www.nycourts.gov/reporter](http://www.nycourts.gov/reporter)

# Identity Theft

- New York enacts: **Security Breach & Notification Act**; December 2006.
- The Act requires government agencies who do business in NY to notify consumers of data security breaches.
- “Private Information”- shall mean personal information and social security number, driver’s license number, and credit card numbers.

# Identity Theft

## **Security Breach & Notification Act**

continued:

The NY Act is similar to California security breach laws which was enacted over two years ago.

Legislation which requires consumer notification of data security breaches has now been approved in 15 states.



# Identity Theft

## **Different Ways Identity Theft Occurs:**

- (1) Stealing – wallets, purses, through your mail; credit card and Bank statements. Records from employers.
- (2) Phishing - thieves pretend to be legitimate companies and or financial institutions and they send to you over the internet spam or messages requesting your personal information.
- (3) Address changes – your billing statements are sent to another location other than your billing address by the thieves completing a “change in address” form.
- (4) Skimming – your debit/credit card numbers are stolen by use of a special storage device when your card is processed.
- (5) Dumpster diving – thieves look through your garbage looking for bills and documents with your personal information on it.

# Identity Theft

## **Be Alert to possible Identity Theft**

### Signs of Identity Theft:

- Unexpected account statements or credit card bills.
- Denial of credit.
- Bills not arriving timely and telephone calls or correspondence regarding purchases you did not make.

### Request a free credit card report from:

- Equifax
- Experian
- TransUnion.

Visit [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or call 1-877-322-8338, a service created by these three companies, to order your free credit reports each year. You also can write: Annual Credit Report Service, P.O. Box 105281, Atlanta, GA 303048-5281.

# Identity Theft

## **Safeguarding Your Personal Information:**

- Keep your personal information at home in a safe place.
- Shred “all” documents that contain personal information especially financial documents.
- Do not carry your Social Security Card in your wallet. Always ask if there is another identifier that can be used for identification.
- Internet Use:
  - Do not give out personal information unless you know who you are dealing with.
  - Do not click on links of unsolicited E-Mails. Ensure privacy by use of anti-spyware, anti-virus software and use of firewalls.
  - Be creative with your password. Do not use the last four digits of your social security number, your birthday or your mothers maiden name.

# Identity Theft

## **Steps To Protect Against Identity Theft:**

- Place a "Fraud Alert": The alert instructs creditors to follow procedures before changes are made to any of your existing accounts or before any new accounts are open.

Telephone anyone of the toll free numbers below to place a 90-day fraud alert and you can also e-mail them:

Trans Union: 1-800-680-7289; [www.transunion.com](http://www.transunion.com)

Experian : 1-888-397-3742; [www.experian.com](http://www.experian.com)

Equifax : 1-800-525-6285; [www.equifax.com](http://www.equifax.com)

- File a police report with your local police. Make sure you get a copy of the police report; or at the very least a docket number.

# Identity Theft

- Close all your accounts that have been effected by the theft and those that may have been fraudulently opened. Request written verification that accounts are closed and debts discharged.
- Telephone each credit card company security department and inform them of your identity theft.
- Website <http://101-identitytheft.com/checklist.html> provides an Identity Theft victim a worksheet that is an excellent tool which organizes reporting steps.

(See Schedule A – Identity Theft Victim Worksheet)

# Identity Theft

- Website <http://www.ftc.gov/idtheft> has available an Identity Theft Affidavit Form (see Schedule B) which can be used when reporting your Identity Theft to all credit card companies.
- Report your Identity Theft to the Federal Trade Commission:
  - Telephone #: 1-877-438-4338
  - On-line : <http://www.ftc.gov/idtheft>
  - By mail : Identity Theft Clearing House  
Federal Trade Commission  
Washington, DC 20580

# Identity Theft



**Check Your Social Security:** Request your benefits estimate statements by completing Form 7004 or by calling the Social Security Administration at: 1-800-772-1213

When you received your statement look for the following:

- Overstatement, Incorrect, or missing earnings (your earnings should agree with each year's W-2 or your tax return)
- Wrong Date of Birth.
- Misspelled name.

If you have any of these problems call the Social Security Fraud Hotline at 1-800-269-0271.

# Identity Theft

## **Identity Theft May Affect Tax Records:**

A thief (possibly an undocumented worker) may use your Social Security Number to get a job. If the thief receives a W-2 and files a Tax Return with the IRS and receives a refund and you then file your Tax Return the IRS believes that your return is a second copy or duplicate. If this occurs the IRS will send you a notice which in part may state:

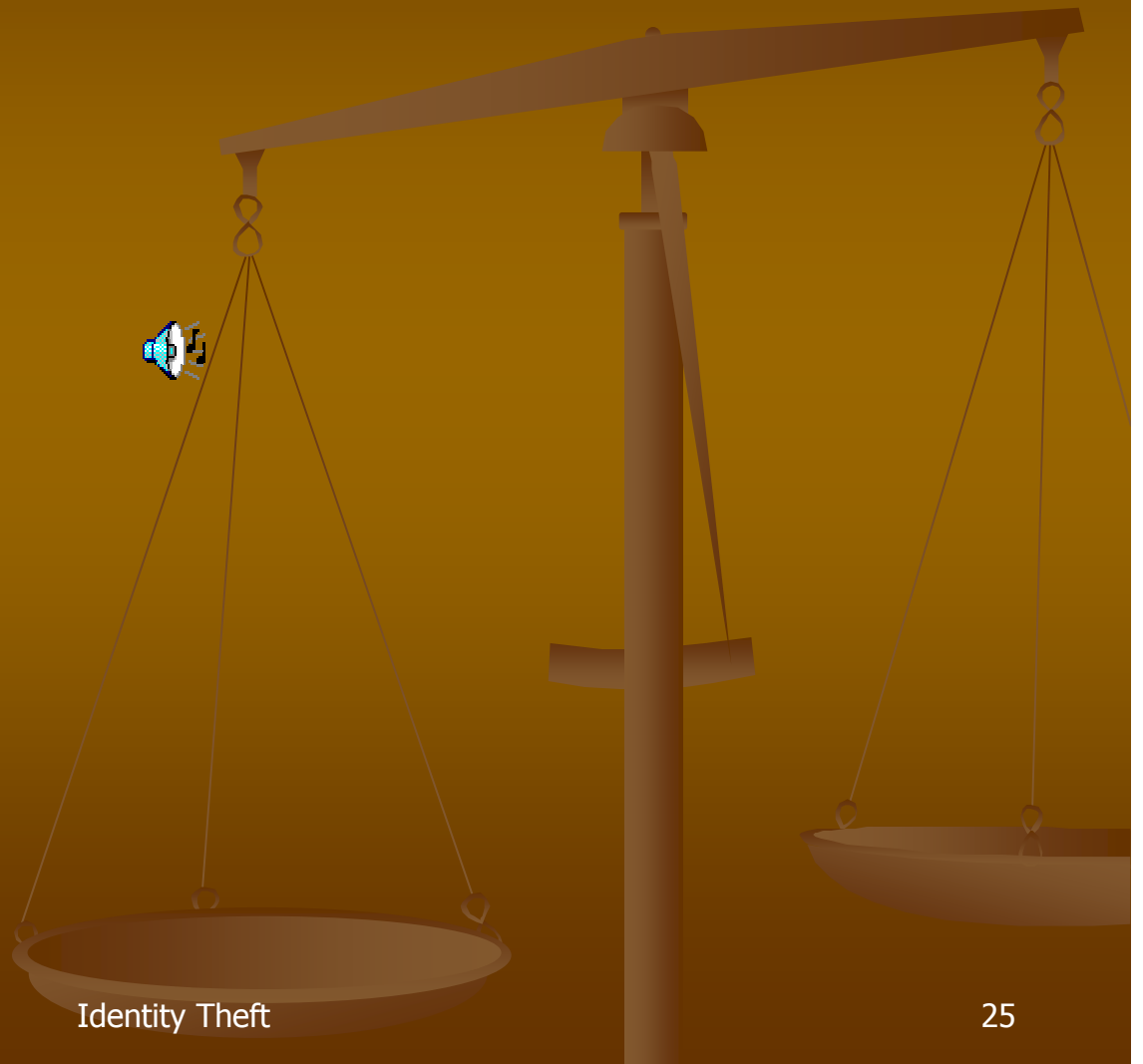
- More than one Tax Return for you was filed, **or**
- IRS records indicate you received wages from an employer unknown to you

Call the IRS immediately and one of the agency's tax examiners will work with you to resolve the problem.



# Identity Theft

- Thank You!



10/1/2007

Identity Theft

25